

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

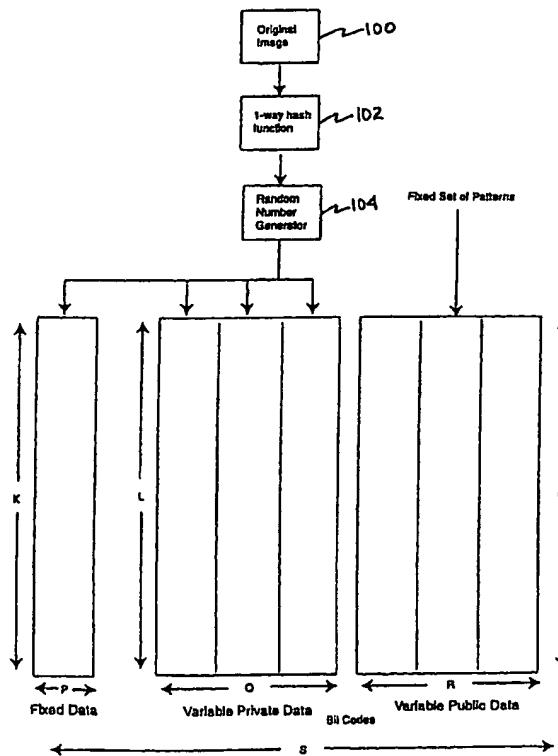
(51) International Patent Classification 6 : <b>G09C 5/00, 1/00</b>	A1	(11) International Publication Number: <b>WO 00/33282</b>
		(43) International Publication Date: <b>8 June 2000 (08.06.00)</b>

(21) International Application Number: <b>PCT/US99/11264</b>	(81) Designated State: <b>JP.</b>
(22) International Filing Date: <b>20 May 1999 (20.05.99)</b>	Published <i>With international search report.</i>
(30) Priority Data: <b>09/201,056</b> 30 November 1998 (30.11.98) US	
(71) Applicant: <b>SIGNAFY, INC. [US/US]; 4 Independence Way, Princeton, NJ 08540 (US).</b>	
(72) Inventors: <b>MILLER, Matthew, L.; 44 Tee-Ar Place, Princeton, NJ 08540 (US). WU, Min; 228A Harrison Lane, Princeton, NJ 08540 (US).</b>	
(74) Agents: <b>GROLZ, Edward, W. et al.; Scully, Scott, Murphy &amp; Presser, 400 Garden City Plaza, Garden City, NY 11530 (US).</b>	

(54) Title: COMBINING MULTIPLE MESSAGES WITH DIFFERENT CHARACTERISTICS FOR WATERMARKING

(57) Abstract

A method for inserting at least two messages into digital data (100) having the steps of: deriving the messages using a hash of the data (102) as a seed to a random number generator (104); representing each of the messages with an individual signal such that all of the individual signals, when combined, do not interfere with one another and each individual signal has its own robustness characteristics; combining the individual signals to create a watermark signal; and inserting the watermark signal into the digital data to be watermarked. Also provided is a method for detecting a target message from digital data containing at least two watermark messages.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Larvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		

COMBINING MULTIPLE MESSAGES WITH  
DIFFERENT CHARACTERISTICS FOR WATERMARKING

5       The present invention relates generally to inserting a watermark into digitized data. Specifically, this invention relates to inserting a combined watermark into digital data, the combined watermark containing at least two messages, each message having different characteristics such as robustness.

10      There are many proposals for watermarking media content, [see *A review of watermarking and the importance of perceptual modeling*, I.J., Cox, Matt Miller, Proceedings of SPIE, Human Vision and Electronic Imaging II, Vol. 3016, pp 92-99, February 1997]. Generally, watermarking is a process whereby a message is inserted 15     into multimedia content by modifying the media data itself, i.e., in the case of imagery, the pixel intensities may be altered in an imperceptible way, but in a manner that is detectable by a computer or other device. We define the difference between the original 20     and watermarked data immediately after watermark insertion as the watermark signal. This signal can be constructed in many different ways. For example, a 25     unique pseudo-random noise (PN) sequence can be used to represent an arbitrarily long message that is determined by using the PN sequence as an index into a database. Alternatively, a n-bit sequence may be directly inserted into an image in a manner whereby each bit is represented 30     by a PN sequence and these n sequences are added or subtracted depending on whether the value of the corresponding bit is zero or one (See United States Patent No. 5,636,292 to Rhoade). Many other methods known in the art are also possible. These different 35     methods have different characteristics with regard to robustness, fidelity, resistance to tampering, such as counterfeiting and collusion attacks, which are described

- 2 -

in more detail subsequently, and requirements at the detector, e.g., secret keys and restricted access to the watermark.

5 It is becoming apparent that users may wish to insert several types of information, e.g., owner identification, buyer identification and copy control information. And different types of information may have different requirements regarding the compromises to be made between  
10 characteristics such as robustness, fidelity, and resistance to tampering. However, in the prior art, all the information encoded by a watermark has been treated equally.

15 There are three significant classes of watermark signal, namely watermark signals that are immune from counterfeiting, watermarks that are resistant to collusion attacks and public watermarks for which no secret information is needed at the detector. These  
20 three classes of watermark signal can possess very different characteristics. For example, a watermark signal that is immune to counterfeiting cannot also be a public watermark.

25 S. Craver et al., *Resolving rightful ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications*, IEEE J. Selected Areas of Communications, 16, 4, 573-586, (1998) (hereinafter "Craver") describes a situation in which rightful ownership cannot be resolved by a straightforward application of watermarking. In particular, a situation is identified in which anyone could claim ownership of a watermarked image through a process whereby a counterfeit watermark is inserted. Craver's solution to this problem  
30 is to use a method called "non-invertible" watermarking. The basic idea behind this method is to construct a watermark based on a non-invertible function of the  
35

- 3 -

original image. An example of a non-invertible function  
is a one-way hash function commonly used in cryptography.  
Such a function takes a string of bits as input and  
outputs a finite output, for example, a 1000-bit output.  
Given the 1000-bit output, it is computationally  
infeasible to determine the corresponding input. Such a  
watermark can only be read by the content owner or  
someone in possession of the original image or its hashed  
key. Thus, a public watermark, i.e., a watermark that  
can be read by anyone, cannot be non-invertible or, at  
least the benefits of non-invertibility are lost since  
all readers must have knowledge of the hashed value.

Another issue to do with tampering with watermarks is  
discussed in Cox et al., *Secure Spread Spectrum  
Watermarking for Multimedia*, IEEE Transactions on Image  
Processing, Vol.6, No.12, pp.1673-1687, 1997. This  
problem occurs when there are many copies of the same  
original image, each copy having a different watermark.  
Then, owners of these copies can collude together in an  
attempt to remove the watermark. For example, a simple  
collusion scheme would be to average together all of the  
available copies. Other more sophisticated methods also  
exist. United States Patent No. 5,664,018 to Leighton  
(hereinafter "Leighton") shows that in such a situation,  
the most robust form of watermark is drawn from a Normal  
Guassian distribution rather than a binary distribution.  
Such an attack would be as effective on either invertible  
or non-invertible watermarks. Unfortunately, Leighton's  
proposal only maximizes the number of copies of an  
original that are needed before the watermarks are  
removed. It does not prevent a collusion attack but  
simply makes it somewhat more difficult. However, in  
practice, the number of copies needed is still relatively  
small.

- 4 -

The present invention is concerned with the broad problem of inserting both owner and buyer identification information into content in as secure a way as possible. What is needed is a robust watermarking system in which some portion of the watermark remains fixed in all watermarked copies of an original and the remaining portion may vary with each copy.

Further, the fixed watermark is constructed from a non-invertible function of the image so that a counterfeiting attack is not possible. The copy-specific portion of the watermark can also be constructed to be non-invertible although some fraction of this might also be invertible to allow anyone to read them.

The present invention provides a watermark signal which can be constructed such that a portion of the data encoded in the watermark signal possesses one set of characteristics while other portions of the data are encoded so as to possess different characteristics.

Accordingly, a method for inserting at least two messages into digital data to be watermarked is provided. The method comprises the steps of: representing each of the messages with an individual signal such that all of the individual signals, when combined, do not interfere with one another and each signal has its own robustness characteristics; combining the individual signals to create a watermark signal; and inserting the watermark signal into the digital data to be watermarked.

Also provided is a method for detecting a target message from digital data containing at least two watermark messages. The method comprises the steps of: extracting a watermark signal from the data, the watermark signal containing an individual signal corresponding to each of the at least two watermark messages; removing all but one

- 5 -

of the individual signals from the watermark signal; and decoding the remaining individual signal to obtain the target message.

5 These and other features, aspects, and advantages of the methods of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawing where:

10 FIG. 1 illustrates a schematic of the insertion method of the present invention.

15 Although this invention is applicable to numerous and various types of digitized data, it has been found particularly useful in the environment of digital video data. Therefore, without limiting the applicability of the invention to digital video data, the invention will be described in such environment.

20 The final watermark that is inserted in a image can be considered to consist of a string of symbols, where each symbol is represented by a pattern and the watermark is constructed by the addition or subtraction of this pattern. For a binary watermark consisting of N-bits, each bit would be represented by a unique pattern and each pattern would be added or subtracted depending on whether the corresponding bit was zero or one. A watermark does not have to contain only binary bits. For example, the non-varying data to be inserted in each copy 25 of an image can be represented by a single pattern. When this pattern is detected, the information associated with the pattern can be determined through a database, which is indexed by patterns.

30 Thus, the general problem is to (i) securely insert R patterns into an image, where I $\geq$ 1 patterns represent copy independent information and R-I patterns may vary with

- 6 -

each copy and (ii) detect these patterns when only a subset may be present in the degraded image.

Figure 1 illustrates the basic ideas behind insertion.  
5 The original image 100 is passed through a one-way hash function 102, such as the NST SHA-1 function, to produce a k-bit key that is image dependent. This key is then used as the seed to a pseudo-random number generator 104. The generator may be binary or continuous and might  
10 provide one of many distributions including uniform and Normal.

K-values from the PN generator are used to form the pattern associated with the copy-independent data. We  
15 assume that the copy-dependent data consists of Q binary bits, though this is not necessary. Each of the Q-bits is represented by an L-dimensional sequence of values from the PN generator. Finally, we assume R additional bits of information, which are represented by a set of M-dimensional values that are not content dependent.  
20

The dimensions of each set of patterns may be equal, i.e.,  $K=L=M$ , and may equal the dimensions of the image. However, in general they need not be equal and may be  
25 considerably less than the dimension of the image, depending on the type of embedding method that is used. For simplicity, we will assume that the Q-bits and R-bits have identical dimension to that of the copy-independent data.  
30

Mathematically, we have  $S=P+Q+R$  patterns that must be embedded in the content. Without loss of generality, we can assume that  $P=1$ , and let A denote the copy-independent pattern. The remaining  $Q+R$  patterns are either added or subtracted, depending on whether their corresponding bit is zero or one. For mathematical convenience, we assume a bipolar bit pattern, i.e.,  
35

- 7 -

values of  $\pm 1$ . Let  $B$  denote the bit pattern to be embedded. Note that  $B$  may also include error correction code bit as well as data bits.

5 M-bit data is coded by error-correction coding to enhance robustness. Two types of linear block codes, namely the Hamming code and Binary BCH code, have been studied [See R.E. Blahut: *Theory and Practice of Data Transmission codes*, 2<sup>nd</sup> edition (draft), 1977; J.G. Proakis: *Digital Communications*, 3<sup>rd</sup> edition, McGraw Hill, 1995; and C.B. 10 Rorabaugh: *Error coding cookbook*, McGraw Hill, 1995]. IN the preferred implementation of the present invention, the following notation of coding is followed:

15               [n,m,d,t]   Linear block codes  
n               -       codeword length in bits,  
m               -       number of data bits,  
d               -       minimal Hamming distance between  
                    codewords, that is, the minimum number  
                    of different bits between codewords,  
20               of         
t               -       maximum number of bit errors within  
                    every n-bit codeword that can be  
                    corrected, with  $d = 2t + 1$ .

25 The Hamming code is one of the simplest error correction codes. It is a linear black code with specification of  $[2^k - 1, 2^k - k - 1, d = 3, t = 1]$ , where  $k$  is a positive integer. There are several common settings of  $k$ , among which [See e.g., ELE539 *Theory and Practice of Channel Coding*, Class Notes, Princeton University, Spring, 1998; 30 R.E. Blahut: *Theory and Practice of Data Transmission Codes*, 2nd edition (draft), 1997; and I.J. Cox, et al.: *Secure Spread Spectrum Watermarking for Multimedia*, IEEE Trans. on Image Processing, Dec.m 1997]. However, the 35 minimal distance of different  $k$  is always three, hence it can always correct one and only one bit error for every  $n$  bits. Meanwhile, the Hamming code has the following

- 8 -

property that is called n perfect code [See R.E. Blahut:  
*Theory and Practice of Data Transmission Codes*, 2nd  
edition (draft), 1997; and ELE539 *Theory and Practice of  
Channel Coding*, Class Notes, Princeton University,  
Spring, Fig. 3, 1998] in an n-dim binary space each

vector is denoted as a point. If a ball is drawn with a  
valid codeword as its center and t as the radius, such a  
ball will enclose all vectors that can be corrected as  
the center codeword vector. The union of all balls of  
hammering code will occupy the whole space without  
leaving any dot outside it. In other words, any vector  
in this space will be associated with one ball and  
corrected to a valid codeword, even though that vector  
may be a noisy version of a codeword in another ball.

Such perfectness is not desirable in multiple-bit  
watermark application since we risk getting bit errors  
after decoding when the watermarked image experiences  
heavy distortions.

Binary BCH coding is more complicated, but a more  
powerful error correction method than the Hamming code.  
This code is used in a variety of practical applications  
due to the existence of computationally efficient and  
easily implemented decoding procedures. The error

correction ability can be chosen from a number of  
settings. Unlike the Hamming code, BCH code has very low  
density for certain specifications. For example, in BCH  
[511,76,t=85] code, the balls described above only  
enclose  $10^{-31}\%$  of points. The points outside will be

detected as invalid codeword but will not be correctable.  
In other words, if the test code vector is very noisy,  
the probability that the detector fails to determine this  
and output an incorrect m-bit vector is  $10^{-33}$ . This is  
desirable for multiple-bit watermarking because we want  
to determine how noisy the received code vector is and to  
avoid correcting a noisy one to a wrong one.

- 9 -

Other powerful error corrections codes are also possible, such as convolutional code and Turbo code [See R.E. Blahut: *Theory and Practice of Data Transmission Codes*, 2nd edition (draft), 1997; J.G. Proakis: *Digital Communications*, 3rd edition, McGraw Hill, 1995; C.B. Rorabaugh; *Error coding cookbook*, McGraw Hill, 1995; and ELE539 *Theory and Practice of Channel Coding*, Class Notes, Princeton University, Spring, 1998].

Returning now to the patterns, let  $C$  denote the  $\{Q+R\}$  patterns, i.e.,  $C$  is a  $L \times (Q+R)$  matrix. The matrix  $C$  can be thought of as a modulation matrix, each column of which represents the chip sequence (to use terminology from spread spectrum communications) for that particular bit. The columns of  $C$  should be orthogonal. This property can be constructed in a variety of ways including Gramm-Schmidt matrix orthogonalization or, for example, by constructing a matrix in which there is only a single non-zero entry in each row. For images and video, this latter case corresponds to the situation in which each bit is encoded in a spatially disjoint region of the image. Another alternative is to generate  $n$   $L$ -dimension orthogonal vectors by randomizing a set of known orthogonal basis obtained in advance. A Hadarmard matrix is an example. It is composed of only +1 and -1 elements and is known to be orthogonal and symmetric. The process is summarized as follows:

- 1) Obtain  $L \times L$  Hadarmard Matrix and randomly select  $n$  column vectors to form an  $L \times n$  matrix.
- 2) Each row of the  $L \times n$  matrix is multiplied by a random binary number (+1 or -1) generated by seeds which can be a function of the original image, hence the set of  $L$ -dimension orthogonal image and the orthogonality is maintained.

- 10 -

- 3) Columns of the randomized  $L \times n$  matrix are normalized such that the resulted matrix  $M$  satisfies  $M'M = I$  (identity matrix).

5 The  $L \times n$  matrix in the first step can be stored beforehand and used for watermarking many images.

Thus, the final signal to be inserted,  $D$  is

10 
$$D = A + C.B$$

The signal  $D$  may be inserted into the image in a variety of well-known ways.

15 To detect this data, it is important to realize that the image containing the watermark may have undergone significant degradations due to normal use and intentional attacks aimed at removing the watermark.  
Consequently, all the patterns that were inserted may not  
20 be present at the time of detection. Thus, we wish to detect each group of patterns independently.

25 In the case where the image noise is not dominant, the primary noise source can be the presence of the other patterns. This situation is common when the original unwatermarked image is used as part of the detection process and can occur in more advanced watermark embedding systems. In particular, we have described three message classes; copy independent/image specific,  
30 copy dependent/image specific and copy dependent/image independent. Each message class has different robustness properties and may or may not be present in the received image. Thus, we need to detect each class independently. However, in the case where the other message groups are  
35 present, these signals appear as noise and, as mentioned earlier, may be the dominant noise source. As such, we would like to minimize their effect on the detection

- 11 -

process.

If  $D'$  denotes the detected signal, then

5            $D' = A + C.B + \text{noise}$

Ignoring the noise term, we can optimally detect for  $A$  by applying Gramm-Schmidt orthogonalization such that

10            $E = D' - C.(D.C^T)$

and then applying a statistical test between the known vector  $A$  and the estimated vector,  $E$ , such as the well known correlation coefficient

15

$$\text{corr} = \frac{E.A}{\sqrt{(A.A)(E.E)}}$$

20           Similarly, to detect the data bits, we first remove any contribution that may be present from  $A$ , i.e.,

$$F = D' A(D.A^T)$$

25           And again perform a statistical test between  $F$  and our best estimate of the pattern of bits present,  $B'$ . Our best estimate of the  $B$  bits is given by

$$B' = (D'.C^T > 0) ? 1 : -1$$

30

i.e. we correlate the received signal with the Q+R patterns. If the correlation value is greater than zero then the corresponding bit is assumed to be 1, otherwise it is -1. Of course, even when no bits are present, we will derive a vector  $B'$  and this is why it is necessary to subsequently test the statistical significance of the estimate. Again, a variety of tests may be applied,

- 12 -

including the correlation coefficient

$$\text{corr} = \frac{F \cdot G_T}{\sqrt{F \cdot F G_T \cdot G_T}}$$

5

where  $G = C \cdot B'$  is the encoded signal for  $B'$ .

It should be noted that the above discussion has  
considered the two copy dependent message groups as one,

10 but it is straightforward to treat these two groups  
separately.

While there has been shown and described what is  
considered to be preferred embodiments of the invention,  
15 it will, of course, be understood that various  
modifications and changes in form or detail could readily  
be made without departing from the spirit of the  
invention. It is therefore intended that the invention  
be not limited to the exact forms described and  
20 illustrated, but should be construed to cover all  
modifications that may fall within the scope of the  
appended claims.

WHAT IS CLAIMED IS:

1       1. A method for inserting at least two messages into  
2       digital data to be watermarked, the method comprising the  
3       steps of:

4               representing each of the messages with an individual  
5       signal such that all of the individual signals, when  
6       combined, do not interfere with one another and each  
7       individual signal has its own robustness characteristics;

8               combining the individual signals to create a  
9       watermark signal; and

10              inserting the watermark signal into the digital data  
11       to be watermarked.

1       2. The method of claim 1, wherein at least one of the  
2       individual signals is based on a non-invertible function  
3       of the digital data.

1       3. The method of claim 1, wherein at least one of the  
2       individual signals is based on an invertible function of  
3       the digital data.

1       4. The method of claim 1, wherein at least one of the  
2       individual signals is based on an invertible function of  
3       the digital data and at least one other of the individual  
4       signals is based on a non-invertible function of the  
5       digital data.

1       5. The method of claim 1, wherein at least one of the  
2       individual signals is copy independent.

1       6. The method of claim 1, wherein at least one of the  
2       individual signals is copy dependent.

- 14 -

1       7. The method of claim 1, wherein at least one of the  
2       individual signals is copy independent and at least one  
3       other of the individual signals is copy dependent.

1       8. The method of claim 1, wherein the individual  
2       signals are orthogonal vectors.

1       9. The method of claim 8, wherein the orthogonal  
2       vectors are generated by Gramm-Schmidt orthogonalization.

1       10. The method of Claim 1, further comprising the step  
2       of encoding each message using an error correction code  
3       prior to representing it as a corresponding individual  
4       signal.

1       11. The method of claim 10, wherein the error correction  
2       code is a BCH code.

1       12. A method for detecting a target message from digital  
2       data containing at least two watermark messages, the  
3       method comprises the steps of:

4               extracting a watermark signal from the data, the  
5       watermark signal containing an individual signal  
6       corresponding to each of the at least two watermark  
7       messages;

8               removing all but one of the individual signals from  
9       the watermark signal; and

10              decoding the remaining individual signal to obtain  
11       the target message.

1       13. The method of claim 12, wherein the removing step is  
2       carried out be Gramm-Schmidt orthogonalization.

1       14. The method of claim 12, wherein the decoding step is

- 15 -

2 carried out by:

3 comparing the remaining individual signal against a  
4 known individual signal corresponding to a possible  
5 content of the target message thereby obtaining a  
6 statistical detection measure; and

7 comparing the statistical detection measure against  
8 a threshold to determine whether the remaining individual  
9 signal decodes into the target message content  
10 represented by the known individual signal.

1 15. The method of claim 14, wherein the known individual  
2 signal is obtained by applying a non-invertible function  
3 to the digital data.

1 16. The method of claim 12, wherein the decoding step  
2 comprises the sub-steps of:

3 multiplying the remaining vector by a demodulation  
4 matrix to obtain a demodulated signal;

5 thresholding elements of the demodulated signal to  
6 obtain a bit pattern; and

7 decoding the bit pattern to obtain the contents of  
8 the target message.

1 17. The method of claim 16, wherein the decoding of the  
2 bit pattern is carried out by error correction code.

1 18. The method of claim 17, wherein the error correction  
2 code is a BCH code.

1 19. The method of claim 12, further comprising the sub-  
2 steps of:

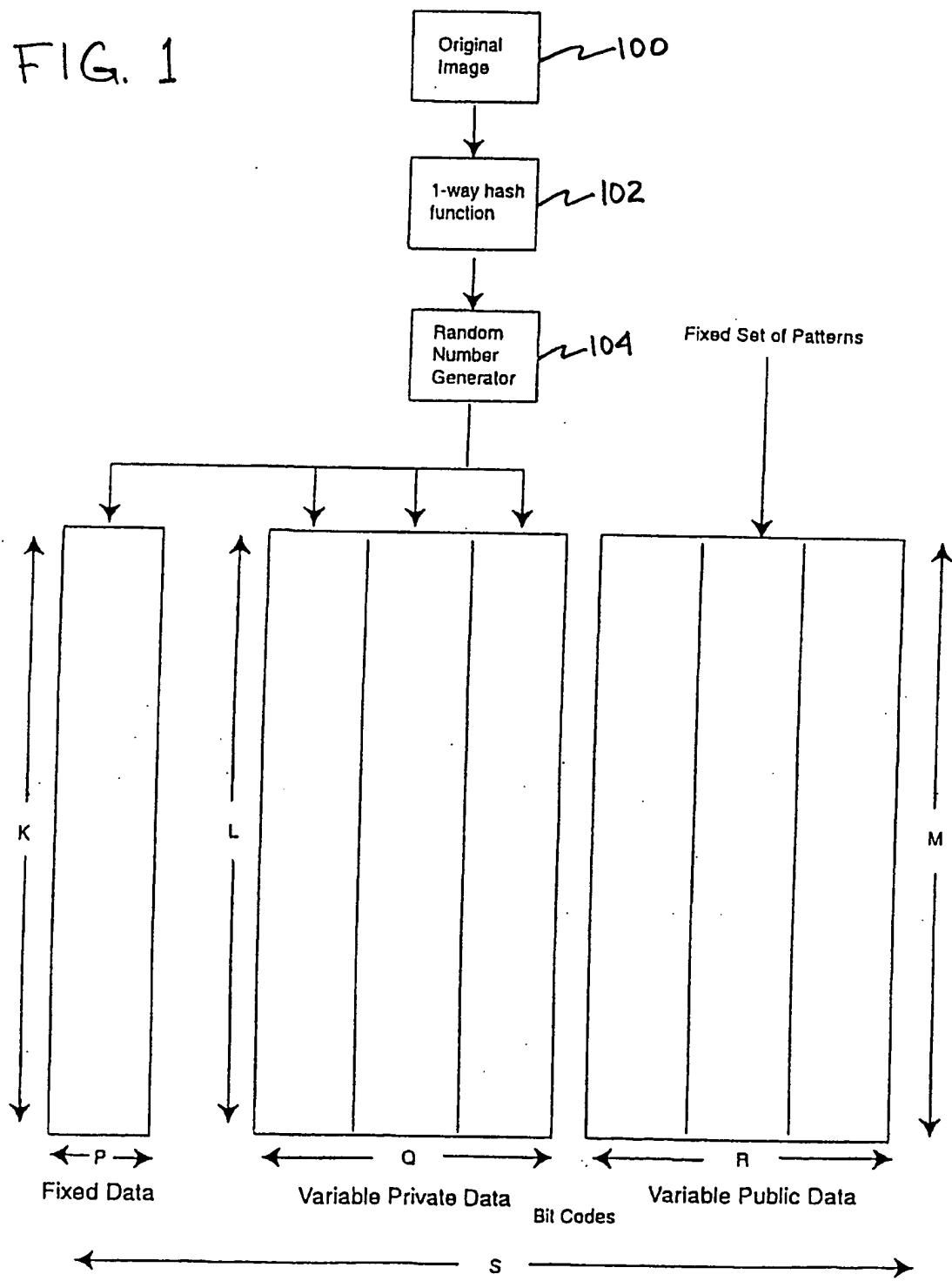
- 16 -

3           re-encoding the target message as an individual  
4       signal;

5           comparing the re-encoded individual signal against  
6       the remaining individual signal thereby obtaining a  
7       statistical detection measure; and

8           comparing the statistical detection measure against  
9       a threshold to determine whether the remaining message is  
10      valid.

FIG. 1



## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US99/11264

## A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) G09C 5/00, 1-00

US CL. 380/54, 4, 25

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/54, 4, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Internet - <http://www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html>

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

USPTO APS "watermark"

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,809,139 A (GIROD et al) 15 September 1998, col. 9, lines 19-23	1, 8, 10-13, 16-18 ----- 2-7, 9, 14, 15, 19
Y		
Y	US 5,613,004 A (COOPERMAN et al) 18 March 1997, col. 16	2-4, 15
Y, P	US 5,905,800 A (MOSKOWITZ et al) 18 May 1999, col. 1, lines 1-36	5-7
A, P	US 5,848,155 A (COX) 08 December 1998, col. 6, lines 1-9	14, 19

 Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	*T*	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
*A* document defining the general state of the art which is not considered to be of particular relevance	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
*E* earlier document published on or after the international filing date	*Y*	document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*&*	document member of the same patent family
*U* document referring to an oral disclosure, use, exhibition or other means		
*P* document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
13 AUGUST 1999	30 SEP 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-0040	Authorized officer  STEVE KABA <i>James R. Matthews</i> Telephone No. (703) 306-4153

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/US99/11264

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	COX et al, Secure Spread Spectrum Watermarking for Multimedia, IEEE Trans. Image Processing, December 1997, Vol. 6, No. 12, Fig. 3 and Eq. 4	14, 19
Y	US 5,319,586 A (GUPTA et al), 07 June 1994, col. 5	9
A	CRAVER et al, Can Invisible Watermarks Resolve Rightful Ownerships?, IBM Research Report, July 1996, RC 20509, Section 5	2-4, 15

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

This Page Blank (uspto)